Revista Ciencia & Tecnología

No. 29, 31 de enero de 2021
ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

La seguridad informática en la adopción del cloud computing en la información del sector industrial

Computer security in the adoption of cloud computing in the information of the industrial sector

Msg. Evelin María Saltos Ramírez [1]
evelinmsr@gmail.com
https://orcid.org/0000-0003-4047-0122
Phd. José Enrique Townsend Valencia[2]
Jose.townsend@htecnologicas.com
https://orcid.org/0000-0001-5319-4425

Recibido: 1/11/2020, Aceptado: 1/11/2020

RESUMEN
Las empresas del sector industrial alimenticio demandan el uso de las tecnologías WEB para mejorar que sus procesos internos sean más eficientes, pero con bajos costos en el uso e implementación de sus infraestructuras de hardware y software encontrando que los servicios de cloud computing proveen las necesidades que requieren. Estas necesidades se ven cuestionadas por la necesidad de un marco de seguridad informático estableciendo la problemática de identificar que factores inciden en la seguridad que se estableció en el estudio de un modelo que permita medir las diferentes variables. Se realizó el estudio de modelos fundamentados en la Norma ISO 27000, en el modelo de Jansen y Grance (2011), en el modelo de Whitman y Mattord (2014) basado en la teoría de John McCumber (1991), en el modelo ISACA (2012) y en el modelo de referencia de (Liu et al., 2011) del Instituto Nacional de Normas y Tecnología que definieron las variables de estudio garantía, gobernanza, servicio, despliegue entre las principales. El estudio fue descriptivo con un enfoque cuantitativo procediendo a la recolección de los datos con encuestas y bases de datos El tipo de investigación fue sistemática y empírica con un corte longitudinal de tendencia en un periodo especifico. Se consideró la técnica estadística para extraer información mediante el análisis de bases de datos públicos de diferentes organismos gubernamentales y no gubernamentales. La selección de la muestra fue a las empresas del sector industrial manufacturero de actividad económica en elaboración de productos alimenticios. El resultado principal del estudio es el planteamiento y evaluación de un modelo con componentes de seguridad informática, la elaboración de una matriz operacional que expone sus variables, dimensiones e indicadores en los factores de seguridad informática que deben ser considerados para el éxito o fracaso al momento de adoptar un modelo cloud computing en las empresas del sector alimenticio.

Palabras clave: cloud computing, seguridad informática, modelo, norma ISO y adopción.

[1] Universidad Tecnológica Empresarial de Guayaquil, Ecuador.
[2] Universidad Nacional Mayor de San Marcos, Perú.

Revista Ciencia & Tecnología

No. 29, 31 de enero de 2021
ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

ABSTRACT
Companies in the food industry demand the use of WEB technologies to improve their internal processes to be more efficient but with low costs in the use and implementation of their hardware and software infrastructures finding that cloud computing services provide the needs that they require. These needs are questioned by the need for a computer security framework establishing the problem of identifying factors that affect the security that was established in the study of a model that allows measuring the different variables. The study of models based on the ISO 27000 standard on the Jansen and Grance model (2011) on the Whitman and Mattord model (2014) based on the John MacCumber theory (1991) on the ISACA model (2012) and in the reference model of (Liu et al., 2011) of the National Institute of Standards and Technology that defined the variables of study guarantee, governance, service, deployment among the main ones. The study was descriptive with a quantitative approach proceeding to the collection of data with surveys and databases. The type of research was systematic and empirical with a longitudinal cut of trend in a specific period. The statistical technique was considered to extract information through the analysis of public databases of different governmental and non-governmental organizations. The selection of the sample was to the companies of the manufacturing industrial sector of economic activity in the elaboration of food products. The main result of the study is the approach and evaluation of a model with computer security components, the elaboration of an operational matrix that exposes its variables, dimensions and indicators in the IT security factors that must be considered for success or failure at the moment to adopt a cloud computing model in companies in the food sector.

Keywords: cloud computing, computer security, model, ISO standard and adoption.

Introducción

El cloud[3] computing en su primera definición por el NIST[4](2009) es un conjunto de recursos tecnológicos compartidos como software, aplicaciones, almacenamiento y servicios que son asignados a demanda de sus costes y sus recursos liberados con un esfuerzo mínimo en la gestión con el proveedor de servicio (Joyanes, 2013) y que están operativos y disponibles en forma ininterrumpida siendo sus características básicas la escalabilidad, aprovisionamiento del servicio, bajos costes y seguridad como factor clave, lo que permite a las empresas adoptar las nuevas tecnologías a un coste reducido generando agilidad y mayor productividad.

La seguridad informática en el cloud computing es un modelo de computación que está creciendo rápidamente en la actualidad existiendo una similitud en el modo que se administra la seguridad con respecto a la tecnología tradicional. El concepto que

[3] CLOUD: Informática en la nube término que surgió en el año 1996 entre la empresa COMPAQ y un grupo de líderes para discutir el futuro de la informática (Mosco, 2014).
[4] NIST: National Institute of Standards and Technology.

No. 29, 31 de enero de 2021
ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

encierra la seguridad de la tecnología cloud computing no modifica el punto de vista de la gestión de seguridad de información relacionado a la prevención, detección, resolución de fraudes y delitos informáticos (Alexander, 2007).

Los principios básicos de confidencialidad, integridad y disponibilidad exigen al cloud computing la garantía de la protección de la información mediante la incorporación de normas, estándares y buenas prácticas de TI en la gestión de la seguridad de la información que permita identificar, gestionar, minimizar y asumir los riesgos potenciales que pueden atentar contra las organizaciones de forma documentada, sistemática estructurada, eficiente para adaptarse a nuevos cambios.

El problema de la investigación busca encontrar la respuesta a: ¿De qué manera incide la seguridad informática en la adopción del cloud computing? y para ello se plantea las siguientes interrogantes que ayudan a dar solución al problema de investigación: ¿Es necesario que exista control de acceso a servicios y aplicaciones en el cloud computing?, ¿Es indispensable para una organización la seguridad y privacidad de la información en todo momento?, ¿Puede existir falla de los servicios y aplicaciones en el cloud computing?, ¿Es posible ser víctimas de ataques informáticos debido al almacenamiento de información confidencial en recursos tecnológicos externos a la organización?.

El estudio tiene como objetivo determinar qué factores influyen en la seguridad informática al momento de adoptar el modelo cloud computing en las pymes del sector industrial siendo los objetivos específicos identificar los modelos de seguridad informáticos y analizar su aplicabilidad en el cloud computing, estableciendo a partir del modelo seleccionado las características de seguridad que deben considerar las empresas del sector industrial para su adopción.

Metodología

En concordancia con la problemática identificada se consideró lo definido en Normas ISO 27000 (2009) que contiene principios básicos de la seguridad para sistemas de información aplicados a cualquier entorno, rescatando las dimensiones que se refiere a disponibilidad, integridad y confidencialidad. En cuanto al cumplimiento de requisitos legales, contractuales y revisiones de seguridad de la información Norma ISO 27002 (2013) Se seleccionó el modelo de Jansen y Grance (2011) que presenta a través del NIST 800-144 la definición en el cloud computing como modelo para permitir acceso desde cualquier lugar, forma cómoda y bajo demanda a recursos compartidos. Del modelo propuesto por Whitman y Mattord (2014), basado en la teoría de John McCumber (1991), se selecciona la Tecnología, considerando las medidas de seguridad a aplicar. Del modelo propuesto por ISACA (2012). Se consideró las responsabilidades que sirve en la comprensión de los riesgos de una empresa, monitoreando el rendimiento y recursos disponibles en la resolución de problemas y finalmente los principios básicos de modelo de referencia de (Liu et al., 2011) presentado por el Instituto Nacional de Normas y Tecnología, NIST y la guía de seguridad para áreas críticas enfocadas a la seguridad en el cloud computing, publicada por el Cloud Security Alliance (2017) en el que a través de la matriz de controles de referencia ofrece una guía de recomendaciones para la gestión de riesgos.

Revista Ciencia & Tecnología

No. 29, 31 de enero de 2021
ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

Tabla 1. Variables causantes en el estudio

	VARIABLES INDEPENDIENTES	DESCRIPCIÓN
SEGURIDAD	(VI01) Garantía	Valora la preservación de la seguridad en los principios de disponibilidad, confidencialidad e integridad
	(VI02) Gobernanza	Valora el control de las políticas, los procedimientos y los estándares aplicados.
	(VI03) Identidad y control de acceso	Valora las protecciones en la autenticación, la autorización y las funciones de control de acceso.
	(VI04) Gestión de riesgos	Mide y valora los riesgos en la empresa y los procedimientos para el monitoreo continuo.
	(VI05) Servicio	Mide el uso de servicios o aplicaciones en cloud computing .
	(VI06) Despliegue	Valora un servicio o aplicación de cloud en entorno Público, Privado, Híbrido o Comunitario.
	(VI07) Cumplimiento	Valora y mide el cumplimiento de estándares, normas o leyes establecida.

Fuente: Elaboración propia

Garantía: Todo proceso dentro de los servicios del cloud computing se mantienen protegidos mediante la medición de sus atributos (ISO,27000):

- Disponibilidad: garantizar el alcance de forma oportuna y precisa.
- Integridad: garantizar que la información no sea alterada en su contenido.
- Confidencialidad: asegurar el control de acceso a la información.

.

Gobernanza: Elemento de mayor nivel debido a que en esta variable se toman las decisiones de caracteres estratégico que afectan a las políticas de seguridad o marco de seguridad (Cárdenas, Martínez & Becerra, 2016).

Identidad y control de acceso: Métodos de autenticación para la identificación de usuarios y mecanismos para el control de accesos, Zhou et al. (2010).

Gestión de riesgos: Mide y valorar los riesgos en la empresa, procedimientos para el monitoreo continuo del estado de seguridad de la información, Responsabilidades (Lategan y Von Solms, 2006).

Servicio: Software, plataforma e infraestructura entregadas al consumidor como un servicio por sus siglas Saas, Iaas y Paas (Lamia & Butrico, 2008)

Despliegue: NIST (2011) divide el modelo de ejecución de un servicio en:

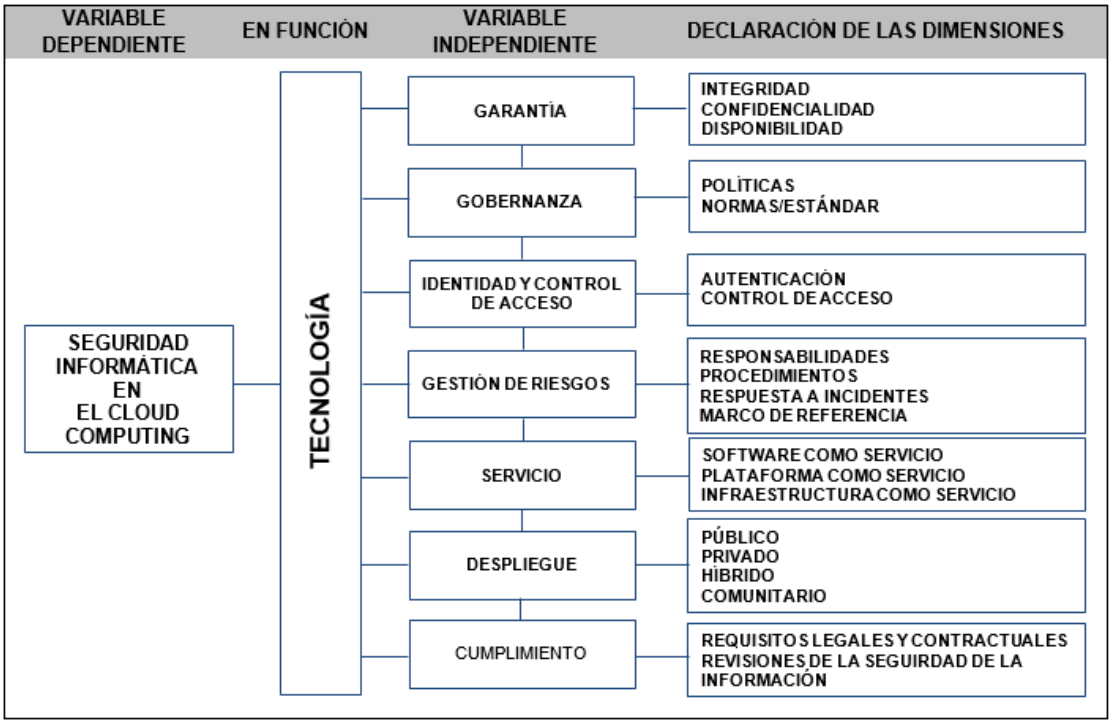
- Nube pública a disposición general o industria en que una organización es propietaria de la venta de servicios.
- Nube privada tiene un servicio de propiedad o de alquiler por una empresa. Nube híbrida combina las características de las nubes públicas y privadas, manejando las responsabilidades de gestión.
- Nube comunitaria es compartida por organizaciones.

Revista Ciencia & Tecnología
No. 29, 31 de enero de 2021
ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

Cumplimiento: Mide el grado de cumplimiento de estándares, normas o leyes a través de Requisitos legales y contractuales y Revisiones de la seguridad de la información (INTECO, 2011).

En la tabla No.2 se describe el modelo general que describe la relación entre la garantía, gobernanza, identidad de control, gestión de riesgo, servicio, despliegue y cumplimiento como variables independientes y la seguridad como variable dependiente.

Tabla 2. Diagrama de variables



Fuente: Elaboración propia

El desarrollo del estudio se caracterizó en dos fases, la primera fase fue la caracterización del modelo luego de una revisión de la literatura con base en la búsqueda de sistemas de seguridad con adopción al cloud computing y la segunda fase conllevó a realizar un análisis de datos referente a las empresas del sector industrial manufacturero. El proceso de esta investigación partió de un estudio descriptivo con un enfoque de la investigación de tipo cuantitativo procediendo a la recolección de los datos con encuestas, bases de datos e información documental analizando la información con métodos estadísticos presentando sus resultados de forma cuantitativa. El tipo de investigación fue sistemática y empírica con un corte longitudinal de tendencia en un periodo especificado.

Esta investigación aplicó el método deductivo ya que inició de una realidad problemática en la seguridad informática y evaluó las variables y dimensiones de un

No. 29, 31 de enero de 2021
ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

modelo teórico que pudo identificar la existencia de factores de éxito o fracaso que determinan la aplicabilidad de la tecnología del cloud computing.

Selección de la muestra y selección de variables
Se realizó un análisis de datos referente a las empresas del sector industrial manufacturero de actividad económica de elaboración de productos alimenticios de la ciudad de Manta, provincia de Manabí con hechos registrados en el 2015, 2016 y 2017 La limitación de esta investigación corresponde a las empresas dedicadas a la actividad económica CIIU C10 afiliadas a la Cámara de Industrias y Cámara de comercio en Manta.

Fuentes de información
Fuentes primarias:
- Revisión de informes emitidos por el INEC desde el 2010 al 2016.
- Información de la Cámara de Industrias y Cámara de Comercio Manta.
- Datos Superintendencia de Compañías, Valores y Seguros del Ecuador.

Fuentes secundarias:
- Información estadística y documental de otras fuentes de información.
- Información de artículos científicos y revistas oficiales.
- Página web del Instituto Nacional de Estándares y Tecnología (NIST), informes de estándares ISO.
- Publicaciones de tesis de investigación científica.
- Revisión literaria sobre el tema.

Técnicas para la recolección de información.
Se consideró tres técnicas para extraer información del estudio: la técnica estadística el análisis de bases de datos públicos de diferentes organismos gubernamentales y no gubernamentales involucrados con la información. La técnica documental recopiló información de las fuentes disponibles, tesis, revistas, páginas web, libros, informes técnicos, artículos científicos. Y finalmente la técnica de investigación de campo mediante el instrumento de encuesta en la que se elaboró 17 preguntas.

Escala aplicada para la evaluación de las variables.
Se empleó la escala de Likert para medir y registrar cada uno de los indicadores recolectados y asociados a las propiedades del fenómeno de investigación. Cada ítem tiene grados de respuestas que van de lo más favorable a lo menos favorable y obtener de la muestra y ser objetiva y precisa.

No. 29, 31 de enero de 2021
ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

Tabla 3. Escala de Likert

ESCALA	CRITERIO	RANGO	
5	En total acuerdo con la seguridad	81%	100%
4	En acuerdo con la seguridad	61%	80%
3	Ni en acuerdo ni en desacuerdo con la seguridad	41%	60%
2	En desacuerdo con la seguridad	21%	40%
1	En total desacuerdo con la seguridad	0%	20%

Fuente: Elaboración propia

Tratamiento de la información

Para el tratamiento de la información numérica se empleó una herramienta estadística la cual ayudó a establecer los resultados estadísticos, permitiendo realizar las comparaciones para comprender el tema de investigación. Se emplearon técnicas de medidas de tendencia central y de posición, como análisis de tabla de distribución de frecuencias, descriptivos, análisis de varianza y tabla de contingencia (tabla cruzada), gráficos de sectores, barras e histograma. Para el caso de las muestras estadísticas se procesó la base de datos con técnicas de selección de datos que brinda el software IBM SPSS.

Resultados y discusión

Desde hace unos años los sistemas de información tradicionales han venido evolucionando e integrando los procesos de toda la empresa para permitir un mejor control de la información, con innovación en tecnología. La finalidad de los sistemas de información es lograr las metas corporativas, la excelencia operacional, desarrollar nuevos productos y servicios, ayudar en la toma de decisiones y obtener una ventaja competitiva.

La seguridad de los sistemas de información se evalúa según los elementos por lo que está compuesta la organización, la tecnología y la administración, que aportan para la funcionalidad de una empresa en procesos. En la tabla No. 4 se detalla los diferentes sistemas de información que se utilizan actualmente y sus funcionalidades utilizadas por las empresas del sector industrial manufacturero C10.

Revista Ciencia & Tecnología

No. 29, 31 de enero de 2021
ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

Tabla 4. Tipos de sistemas de información aplicables al cloud computing

SISTEMA DE INFORMACIÓN	DESCRIPCIÓN
Sistemas de planificación de recursos empresariales (ERP)	Integran los procesos de negocios en manufactura y producción, finanzas y contabilidad, ventas y marketing y recursos humanos en un solo sistema de software. Cuentan con un conjunto de módulos de software integrados y una base de datos central que permite compartir datos entre muchos procesos de negocios y áreas funcionales diferentes en toda la empresa.
Sistemas de administración de relaciones con el cliente (CRM)	Proveen información para coordinar todos los procesos de negocios que tratan con los clientes en ventas, marketing y servicio para optimizar los ingresos, la satisfacción de los clientes, ayuda a las empresas a identificar, atraer y retener los clientes más rentables; a proveer un mejor servicio a los consumidores existentes; y a incrementar las ventas.
Sistemas de administración de la cadena de suministro (SCM)	Ayuda a administrar las relaciones con los proveedores, empresas de compras, distribuidores y compañías de logística a compartir información sobre pedidos, producción, niveles de inventario, y entrega de productos y servicios, de modo que puedan surtir, producir y entregar bienes y servicios con eficiencia.
Sistemas de administración del conocimiento (KMS)	Administran los procesos para capturar y aplicar el conocimiento y experiencia. Estos sistemas recolectan todo el conocimiento y experiencia relevantes en la empresa, para hacerlos disponibles en cualquier parte, enlazan a la empresa con fuentes externas de conocimiento.
Sistemas de procesamiento de transacciones (TPS)	Efectúan y registran las transacciones diarias de rutina necesarias para realizar negocios.
Sistemas para inteligencia de negocios (BIS)	Se refiere a los datos y herramientas de software para organizar, analizar y proveer acceso a la información para ayudar a la toma decisiones más documentadas, incluyen los Sistemas de procesamiento de transacciones (TPS), Sitemas de información gerencial (MIS), Sistemas de soporte de decisiones (DSS), Sistemas de apoyo a ejecutivos (ESS)
Sistemas específicos	Muchos sistemas no son clasificables y por esto se llaman sistemas específicos o a medida. Una gestión de ganado, un control de stock, un sistema de facturación electrónica, enre otros. Son específicos porque fueron hechos para atender a una situación específica y no a toda la empresa como ocurre con el ERP.

Fuente: Elaboración propia

En la tabla No.5 se visualiza los diferentes tipos de sistemas de información que utilizan las empresas del sector industrial manufacturero, actividad económica CIIU 10.

Revista Ciencia & Tecnología

No. 29, 31 de enero de 2021
ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

Tabla 5. Sistemas de información por empresas

INDUSTRIA MNUFACTURERA CIIU 10		Sistemas (ERP)	Sistemas (CRM)	Sistemas (SCM)	Sistemas (KMS)	Sistemas (TPS)	Sistemas (BIS)	Sistemas específicos
C1020.02	PREPARACIÓN Y CONSERVACIÓN DE PESCADO, CRUSTÁCEOS SUMERGIDO EN SALMUERA Y ENLATADO.	✓	✓	*	*	*	*	✓
C1020.02	PREPARACIÓN Y CONSERVACIÓN DE PESCADO, CRUSTÁCEOS SUMERGIDO EN SALMUERA Y ENLATADO.	✓	✓	*	*	*	*	✓
C1020.02	PREPARACIÓN Y CONSERVACIÓN DE PESCADO, CRUSTÁCEOS SUMERGIDO EN SALMUERA Y ENLATADO.	✓	✓	*	*	*	*	✓
C1020.01	PREPARACIÓN Y CONSERVACIÓN DE CAMARÓN Y LANGOSTINOS MEDIANTE EL CONGELADO, ULTRACONGELADO SECADO.	✓	✓	*	*	*	*	✓
C1010.21	PREPARACIÓN Y CONSERVACIÓN DE CARNE MEDIANTE: DESECACIÓN, SALADURA, AHUMADO, ENLATADO.	✓	✓	*	*	*	*	✓
C1080.02	FABRICACIÓN DE ALIMENTOS PREPARADOS PARA ANIMALES DE GRANJA.	*	✓	*	*	*	*	✓
C1020.02	PREPARACIÓN Y CONSERVACIÓN DE PESCADO, CRUSTÁCEOS SUMERGIDO EN SALMUERA.	✓	✓	*	*	*	*	✓
C1071.01	ELABORACIÓN DE PAN Y OTROS PRODUCTOS DE PANADERÍA.	*	*	*	*	*	*	✓
C1040.11	ELABORACIÓN DE ACEITES CRUDOS VEGETALES (SIN REFINAR).	*	*	*	*	*	*	✓
C1061.11	MOLIENDA DE CEREALES, PRODUCCIÓN DE HARINA.	*	*	*	*	*	*	✓
C1020.01	PREPARACIÓN Y CONSERVACIÓN DE CARNE MEDIANTE: DESECACIÓN, SALADURA, AHUMADO, ENLATADO.	*	*	*	*	*	*	✓
C1071.02	ELABORACIÓN DE PASTELES Y OTROS PRODUCTOS DE PASTELERÍA.	*	*	*	*	*	*	✓
C1030.11	ELABORACIÓN DE ALIMENTOS COMPUESTOS (MEZCLA) PRINCIPALMENTE DE FRUTAS LEGUMBRES.	*	*	*	*	*	*	✓
C1020.04	ELABORACIÓN DE PRODUCTOS DE PESCADO COCINADO.	*	*	*	*	*	*	✓
C1020.02	PREPARACIÓN Y CONSERVACIÓN DE PESCADO, CRUSTÁCEOS SUMERGIDO EN SALMUERA.	*	*	*	*	*	*	✓

Fuente: Elaboración propia

Correlación de las variables cualitativas

Se estableció la asociación aplicando tablas de contingencia recolectando las variables cualitativas a relacionar, inversión en tecnología y el de software de seguridad, determinando un grado de asociación lineal, estableciendo la relación entre la integridad con el uso de la firma digital con algún tipo de software de seguridad con dio como resultado 53,3% tal como se muestra en la tabla No.12.

Revista Ciencia & Tecnología

No. 29, 31 de enero de 2021
ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

Tabla 6. Correlación de variables

tic17_firma_digital*tic135_seguridad tabulación cruzada

			tic135_seguridad		
			SI	NO	Total
tic17_firma_digital	SI	Recuento esperado	8,7	4,3	13,0
		% dentro de tic17_firma_digital	61,5%	38,5%	100,0%
		% dentro de tic135_seguridad	80,0%	100,0%	86,7%
		% del total	53,3%	33,3%	86,7%
	NO	Recuento esperado	1,3	,7	2,0
		% dentro de tic17_firma_digital	100,0%	0,0%	100,0%
		% dentro de tic135_seguridad	20,0%	0,0%	13,3%
		% del total	13,3%	0,0%	13,3%
Total		Recuento esperado	10,0	5,0	15,0
		% dentro de tic17_firma_digital	66,7%	33,3%	100,0%
		% dentro de tic135_seguridad	100,0%	100,0%	100,0%
		% del total	66,7%	33,3%	100,0%

Fuente: Elaboración propia

Prueba de chi cuadrado.- El estadístico observado 1,154 tiene una distribución de 1 grado de libertad (gl= 1) con una probabilidad de asociación de significancia de 0,283, lo que indica que existe una relación de independencia entre la integridad con la firma digital y el software de seguridad.

Tabla 7. Relación de variables

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	1,154[a]	1	,283
Corrección de continuidad[b]	,072	1	,788
Razón de verosimilitud	1,772	1	,183
Prueba exacta de Fisher			
Asociación lineal por lineal	1,077	1	,299
N de casos válidos	15		

a. 3 casillas (75,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,67.

b. Sólo se ha calculado para una tabla 2x2

Fuente: Elaboración propia

Análisis estadístico de frecuencias

Se aplicó el análisis estadístico de frecuencias determinando el porcentaje del uso de la firma electrónica como mecanismo para mantener la integridad de la información, se tomó la dimensión INTEGRIDAD como variable extraída de la base de datos del Instituto

Revista Ciencia & Tecnología

No. 29, 31 de enero de 2021
ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

Nacional de Estadísticas y Censos referente al recurso Participación de Tecnologías de Información y Comunicaciones en empresas por sectores económicos año 2015.

Tabla 8. Frecuencia la variable

Utilizó su empresa firma digital en comunicaciones enviadas? Solo si dispone de internet o intranet

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	SI	13	86,7	86,7	86,7
	NO	2	13,3	13,3	100,0
	Total	15	100,0	100,0	

Fuente: Elaboración propia

En la tabla 9 se identifica los resultados de la tabla cruzada en donde se utilizó el uso de la firma electrónica y software de seguridad representando un porcentaje de 53,3% de utilización considerando las dos variables, y según la escala de Likert tiene un criterio de 3 puntos que significa que se está NI EN ACUERDO NI EN DESACUERDO con la seguridad considerando el principio de integridad mediante el uso de la firma electrónica y software de seguridad.

Tabla 9. Relación de integridad aplicada

tic135_seguridad*tic17_firma_digital tabulación cruzada

			Utilizó su empresa firma digital en comunicaciones enviadas? Solo si dispone de internet o intranet		
			SI	NO	Total
Software Libre - Otras, como sofware de seguridad (p.e. Open SSL, SSH), plataformas de aprendizaje (Moodie)	SI	Recuento	8	2	10
		% del total	53,3%	13,3%	66,7%
	NO	Recuento	5	0	5
		% del total	33,3%	0,0%	33,3%
Total		Recuento	13	2	15
		% del total	86,7%	13,3%	100,0%

Los porcentajes y los totales se basan en respuestas.

Fuente: Elaboración propia

Likert sobre las 20 variables con sus respectivas dimensiones e indicadores. Se tomó para la investigación que el nivel de aceptación o incidencia de las variables debe ser superior o igual a 61% basándose en la escala de Likert.

Revista Ciencia & Tecnología

No. 29, 31 de enero de 2021
ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

Tabla No. 10 OPERACIONALIZACIÓN Y RESULTADOS

VARIABLE ID	NO.	DIMENSIÓN	DESCRIPCIÓN DE LA VARIABLE	INDICADOR	RESULTADO INCIDENCIA
Garantía	1	Integridad	Medidas aplicadas para asegurar la integridad de la información	% Control de permisos de usuarios	53,30%
	2	Confidencialidad	Disponibilidad de una intranet como medida en los roles de usuarios	Roles de usuarios	62,00%
	3	Disponibilidad	Disponibilidad de un servicio	Porcentaje de disponibilidad Tiempo promedio de falla Tiempo promedio de recuperación	93,50%
Gobernanza	4	Políticas	Políticas de seguridad informática	Políticas aplicadas/Total Políticas adecuadas	80%
	5	Normas/Estándar	Normas de seguridad informática	Número de norma/estándar para el cloud	86,70%
Identidad y control de acceso	6	Autenticación	Métodos de autenticación	Detalle de medidas empleadas como método de autenticación	66,70%
	7	Control de Acceso	Mecanismos de control de acceso	Se cuenta o no con conexión a intranet, control de acceso, firmas digitales	86,70%
Gestión de riesgos	8	Responsabilidades	Personal especialistas en el uso TIC	Cantidad de personas que son especialistas en el uso de TIC.	86,70%
	9	Procedimientos	Técnicas y procedimientos	Cantidad de procedimientos como medida en la gestión de riesgos	86,70%
	10	Respuesta a incidentes	Descripción de actividades como respuesta a incidentes en la gestión de riesgos	Cantidad de procedimientos para respuesta de incidentes	86,70%
	11	Marco de referencia	Descripción del marco de referencia	Tipos de marco de referencia	86,70%
Servicio	12	Plataforma como servicio	Propiedad de servicio como plataforma	Cantidad de aplicaciones que se pueden ejecutar y desarrollar sobre el cloud	20,00%
	13	Software como servicio	Propiedad de servicio como software	Cantidad de Software como servicio	68,70%
	14	Infraestructura como servicio	Propiedad de servicio como infraestructura	Tipos de aplicaciones o servicios	22,20%
Despliegue	15	Público	Importancia del despliegue en la nube pública	Recursos asociados automatizados	66,70%
	16	Privado	Importancia del despliegue en la nube privada	Porcentaje de recursos con arrendamientos	6,70%
	17	Híbrido	Importancia del despliegue en la nube híbrida	Cantidad de elementos compartidos	6,70%
	18	Comunitario	Importancia del despliegue en la nube comunitaria	Porcentaje de recursos compartidos	53,30%
Cumplimiento	19	Requisitos legales y contractuales	Requisitos legales	Controles de requisitos legales y contractuales	86,70%
	20	Revisiones de la seguridad de la información	Controles de revisiones de seguridad de información	Porcentaje de revisión de cumplimiento	6,70%

Fuente: Elaboración propia

Se aplicó la escala de Likert sobre las 20 variables con sus respectivas dimensiones e indicadores. Se tomó para la investigación que el nivel de aceptación o incidencia de las variables debe ser superior o igual a 61% basándose en la escala de Likert.

Se observa que 12 indicadores se encuentran en los niveles de aceptación de la seguridad y el resto de los indicadores que representa el 35% requieren de atención. Entre los indicadores que requieren atención inmediata se encuentran garantizar la integridad, confidencialidad, evaluar la plataforma e infraestructura como servicio en un despliegue público, privado y comunitario según las diferentes aplicaciones que se utilicen.

Conclusiones

El objetivo planteado en la investigación identificó la relación de los modelos de seguridad informática fundamentados por los principios básicos de modelo de referencia de (Liu et al., 2011) presentado por el Instituto Nacional de Normas y Tecnología, además se tomó información de la guía de seguridad para áreas críticas

No. 29, 31 de enero de 2021
ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

enfocadas a la seguridad en el cloud computing, publicada por el Cloud Security Alliance (2017) y la aportación de otros modelos.

El proceso de evaluación del modelo planteado mediante las veinte variables en función de la aplicabilidad de la tecnología del cloud computing se realizó mediante pruebas estadísticas, análisis relativos y cálculos porcentuales estableciendo una escala de valor por cada dimensión a partir de su resultado. La aplicación de la escala ayudó a identificar las dimensiones consideradas como un factor crítico que incide en la seguridad informática de los sistemas en cloud computing.

Se evidenció que existen debilidades en las medidas para garantizar la seguridad informática, lo demuestra la dimensión INTEGRIDAD, donde el valor de 3 puntos representa una ponderación de 53,3% asimismo lo demuestra la dimensión CONFIDENCIALIDAD con un valor de 3 puntos que representa una ponderación del 60%, ocupando en la escala una relación media en comparación a las 20 variables.

Para la variable SERVICIO se identificó dos dimensiones con puntaje bajo en relación a la escala aplicada, las cuales son *Plataforma como servicio* e *infraestructura como servicio*.

Según la valoración de la variable DESPLIEGUE la cual refiere al tipo de implementación donde se ejecuta un servicio o aplicación, se consideró tres dimensiones PÚBLICO, PRIVADO y COMUNITARIO representando sus resultados como una relación media en la escala de Likert.

También se determinó la correlación de las variables que permitió determinar la correspondencia de los datos recopilados, tomando para efecto del análisis las dimensiones INTEGRIDAD y CONTROL DE ACCESO mediante pruebas estadísticas de tablas de contingencia, CHI cuadrado, coeficiente de contingencia (Karl Pearson) y coeficiente de Cramer, en el cual se midió el grado de asociación lineal.

Se estableció en sus resultados que dentro de los entornos de tecnologías de la información está presente los riesgos informáticos debido a las vulnerabilidades y amenazas determinando que existen debilidades para garantizar la seguridad y la privacidad de la información en la adopción de la tecnología cloud computing para las empresas del estudio.

Referencias

Alexander, A. (2007). *Diseño de un Sistema de gestión de seguridad de información, óptica 27001.* Bogotá. Editorial Alfaomega.

Aguilera, L. P. (2010). *Seguridad Informática*. Disponible en https://books.google.es/books?hl=es&lr=&id=Mgvm3AYIT64C&oi=fnd&pg=PA1&dq=bell+seguridad+inofrmatica&ots=PpsqOyBDX0&sig=CK9G8FTiTTITGBUUUxpEHuManUM#v=onepage&q=bell&f=false [consulta: 20-2-2019]

Areitio, B. (2008). *Seguridad de la Información Redes, informática y sistemas de información*. Madrid: España. Editorial Paraninfo S.A.

No. 29, 31 de enero de 2021
ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

Blacio, K. (2015). *Análisis y entrega de un plan para la gestión de seguridad de la información para empresas multinacionales de seguros con presencia en Ecuador.* Disponible en Repositorio Institucional de la Universidad de Guayaquil: http://repositorio.ug.edu.ec/handle/redug/11729 [consulta: 10-9-2018]

Cárdenas, L., Martínez, H..& Becerra, L. (2016). *Gestión de seguridad de la información: revisión bibliográfica*. El profesional de la información, v. 25, n. 6, pp. 931-948. Disponible en https://doi.org/10.3145/epi.2016.nov.10 [consulta: 19-4-2019]

Cabrera, A. (2013). *Estudio para implementación de servicios de data. Universidad de Cuenca*. Disponible en http://dspace.ucuenca.edu.ec/ bitstream/123456789/4667/1/Tesis.pdf [consulta: 11-12-2018]

De Pablos C.& López, J. & Martín, S & Medina, S. (2004). *Informática y Comunicaciones en la empresa*. Madrid, España. Editorial ESIC.

Casasola, R & Maqueo, R.&, Molina, R. & Moreno, G.& Recio, G. (2014). *La nube: nuevos paradigmas de privacidad*. Obregón: México. Editorial CIDE.

Comité de Seguridad de la Información. (2016). *Esquema gubernamental de seguridad de la Información EGSI*. Disponible en https://www.politica. gob.ec/wp-content/uploads/2017/04/EGSI.pdf [consulta: 9-11-2018]

CSA, C. S. (2011). Security Guidance for Critical Areas of Focus in Cloud Computing, V3.0. Disponible en http://www.cloudsecurityalliance.org/ guidance/csaguide.v3.0.pdf. [consulta: 2-6-2018]

Denning, P. (1971). *Third Generation Computer Systems.* New York. Editorial ACM Computing Surveys.

Echenique J. (1990). *Auditoría Informática.* México. Editorial McGraw-Hill.

Gonzáles L. (2016). *Aspectos de seguridad informática en la utilización de cloud Computing.* Recuperado de http://hdl.handle.net/10596/6173

Grance, T. & Mell, P. (2011). *The NIST Definition of Cloud - Recommendations of the National Institute. NIST.* Disponible en http://dx.doi.org /10.6028/NIST.SP.800-145. [consulta: 2-2-2018]

Johnston, S. (2004). *Modeling security concerns in service-oriented architectures*. Disponible en https://pdfs.semanticscholar.org/4c59/4dbd2c4 5cd6779551f3961174053c59b78b9.pdf [consulta: 15-5-2018]

Joyanes, A. (2013). *Computación en la nube. Notas para una estrategia española en cloud computing*. Revista del Instituto Español de Estudios Estratégicos. Disponible en https://cover.vectorsf.net/index.php/ieee/ article/view/10. [consulta: 13-6-2018]

Landwher, E. (1981). *Formal model for computer security.* Computing Surveys. Vol 13. No.3. pp 247-278

Liu, F.& Tong, J.& Mao, J.& Bohn, R., Messina, J., Badger, L. y Leaf, D. (2011). *NIST Cloud Computing Reference Architecture*. Disponible en https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf. [consulta: 15-5-2018]

Medina F. (2011). *Arquitectura y Modelos de Seguridad*. Disponible en http://seguridad.capacitacionentics.com/2012-1-Seguridad_Informatica_ Tema3.pdf. [consulta: 12-5-2018]

Mieres, J. (2009). *Ataques Informáticos Debilidades de seguridad comúnmente explotadas*. Disponible en https://www.evilfingers.net/publications/white_AR/ 01_Ataques_informaticos.pdf [consulta: 10-7-2018]

No. 29, 31 de enero de 2021
ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

Orantes, S., Zavala,A. & Vasquez, G.(2016). Análisis de las implicaciones de seguridad en la adopción del Cómputo en la Nube para las PYMES en México. Memorias de la Décima Quinta Conferencia Iberoamericana en Sistemas, Cibernética e Informática.
Disponibles en http://www.iiis.org /CDs2016 /CD2016Summer/papers/CA523FW.pdf [consulta: 3-3-2019]

Whitman, M. M. (2014). Management of Information Security Forth Edition. Standford. Editorial Cengage learning.

Zhou, M., Zhang, R.. Xie, W., Qian,W.&; Zhou, A. (2010). *Security and privacy in cloud computing: A survey". In: SKG'10 Procs of the 2010 6th intl conf on semantics, knowledge and grids.* Disponible en https://doi.org/10.1109 /SKG.2010.19 [consulta: 24-5-2019]